UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

CONSUMER FINANCIAL PROTECTION BUREAU, Plaintiff, v. ACTIVE NETWORK, LLC, Defendant.	Case No. 4:22-cv-00898-ALM

STIPULATED ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

I. Purpose

This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules.

II. Preservation of ESI

The parties acknowledge that they have an obligation to take reasonable and proportional steps to preserve all potentially discoverable information in the party's possession, custody, or control. With respect to ESI preservation, the parties agree as follows:

A. Pursuant to Fed. R. Civ. P. 26 and 37(e), the parties shall preserve all discoverable ESI in their possession, custody, or control. Each agrees to produce ESI in a timely manner, cooperate on the production of ESI, and to meet and confer to resolve disputes, pursuant to Local Rule CV-7(h).

B. The parties have an ongoing duty to supplement discovery responses with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made, unless excluded under V below.

C. If a party believes in good faith that categories of ESI need not be preserved because it is not reasonably accessible or otherwise, it will inform the other party. If a party is not in agreement that such ESI need not be preserved, the parties agree to confer in an attempt to reach agreement on those categories.

III. Custodians and Review

A. Custodians. As part of the discovery process, the parties agree to confer with each other to determine whether to limit the number of custodians for which ESI will be collected, including discussion of tiered collection if warranted.

B. Technology-Assisted Review. Either party may use technology-assisted review, computer learning, analytics, or predictive coding to identify potentially responsive documents. If any party employs any process based on computer-assisted learning or any similar technology, it should ensure that the person responsible for conducting or supervising the review has substantial knowledge of the issues in this case.

IV. Production Format

Both parties shall produce all documents according to the Bureau's Document Submission Standards, attached to this Stipulated Order except that Active will not include two data fields that would contain the same information as other fields to be produced. Active will not produce the "Source" field as any available source information can be found in the "Original Folder Path" field, and Active will not produce "Parent_ID" as family information can be found in "Production Begin Attach" and "Production End Attach" fields."

V. Privileged and Protected Documents

For each document, tangible thing, or ESI withheld, in whole or in part, based on an asserted claim of privilege or protection, the party asserting the privilege must produce a privilege log.

For electronic documents, each party may opt at its own discretion to create privilege logs using one of the methods below. For paper documents, each party shall create privilege logs using the standard privilege log. No matter the method of generating a privilege log that is chosen, the producing party must produce privilege logs on a rolling basis within twenty-eight days of each document production, rather than at the end of discovery.

A. Automated (Metadata) Log. An automated privilege log will be generated from the following metadata fields, to the extent they exist, as electronic metadata associated with the original electronic documents.

1. SUBJECT
2. FILE NAME
3. AUTHOR
4. SENDER/FROM
5. RECIPIENTS/TO
6. CC
7. BCC
8. SENT DATE TIME
9. RECEIVED DATE TIME
10. FILE CREATED DATE TIME
11. FILE LAST MODIFIED DATE TIME

With respect to the SUBJECT OR FILENAME fields, the producing party may substitute a description of the communication where the content of these fields may reveal privileged information but must indicate that the fields have been revised. Parties shall include a field with information on privilege type, the basis for the privilege assertion, and whether the document has been produced with redactions.

Should the receiving party in good faith have reason to believe a particular entry on the Automated Log does not reflect a privileged document, the parties will confer and the receiving party may request and the producing party shall produce a Standard Log for that entry within fourteen days of the request, or within such other reasonable time as the parties may agree or the Court may order.

B. Categorical Log. A categorical privilege log will include at least these fields: authors/senders/from; recipients/to; date range; privilege types; and a description sufficient to identify the subject of the documents within each category and the basis for the privilege assertions. The parties reserve the right to challenge the adequacy of a categorical log to the extent they believe that it fails to enable them to assess the claim of privilege.

C. Standard Log. A standard privilege log will include at least these fields: author/sender/from; recipients/to; cc; bcc; date; privilege types; and a description sufficient to identify the subject of the document and the basis for the privilege assertion.

D. Beginning with the date the complaint was filed, parties need not note on a privilege log nor produce any documents exchanged with counsel or among counsel (including Bureau counsel) and employees or agents working on counsel's behalf directly related to this litigation such as investigators, paralegals, analysts, information technology and litigation support staff, or litigation support vendors.

VI. Modification

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

IT IS SO ORDERED.

SIGNED this 7th day of October, 2024.

AMOS L. MAZZANT
UNITED STATES DISTRICT JUDGE

CONSUMER FINANCIAL PROTECTION BUREAU | JULY 2021

Discovery Requests Document Submission Standards

CFPB Office of Enforcement

Discovery Document Submission Standards

This document describes the technical requirements for producing electronic document collections to the Bureau of Consumer Financial Protection ("the Bureau")'s Office of Enforcement. All documents shall be produced in complete form, in color when necessary to interpret the document, unredacted unless privileged, and shall not be edited, cut, or expunged. These standards must be followed for all documents you submit in response to all discovery requests. Any proposed file formats other than those described below must be discussed with the legal and technical staff of the Bureau's Office of Enforcement prior to submission.

A. Transmittal Instructions

1) A cover letter should be included with each production. The following information should be included in the letter:
   a) Name of the party making the production and the date of the discovery request to which the submission is responsive.
   b) List of each piece of media (hard drive, thumb drive, DVD or CD) included in the production (refer to the media by the unique number assigned to it, see ¶ 4)
   c) The Bates Range (and any gaps therein)
   d) The specification(s) or portions thereof of the discovery request to which the submission is responsive.
2) Documents created or stored electronically MUST be produced in their original electronic format, not converted to another format such as PDF.
3) Transmittal Methods
   a) Extranet

      The Extranet is the Bureau's secure file transfer solution that is used to receive productions from third parties via a web-based FTPS protocol utility. Instructions on how to access the Extranet and corresponding credentials are provided upon request. When utilizing the Extranet, the following policies must be adhered to:
      i) Directories: The system does not support uploading directories (folders). To upload a directory, please compress (or zip) and upload the zipped container.
      ii) Size: Maximum 2 GB per file or container. Larger productions should be split across multiple 2 GB zipped containers.
      iii) Quantity: There is no limit to how many files or containers can be uploaded simultaneously.
      iv) File types: A list of prohibited file types is available in Appendix B.
   b) Physical Media

      The Bureau recognizes that some conditions of environment or data format may restrict production eligibility for transmittal via the Extranet. Such productions may be produced on CD, DVD, USB thumb drive, or hard drive; use the media requiring the least number of deliverables.
      i) Magnetic media shall be carefully packed to avoid damage and must be clearly marked on the outside of the shipping container:
         (1) "MAGNETIC MEDIA – DO NOT USE METAL DETECTOR"
         (2) "MAY BE OPENED FOR POSTAL INSPECTION"
      ii) CD-R CD-ROMs should be formatted to ISO 9660 specifications;
      iii) DVD-ROMs for Windows-compatible personal computers are acceptable;

iv) USB 2.0 thumb drives for Windows-compatible personal computers are acceptable;
v) USB 3.0 or USB 3.0/eSATA external hard disk drives, formatted in a Microsoft Windows-compatible file system (FAT32 or NTFS), uncompressed data are acceptable.
vi) Physical media should be delivered via overnight delivery service or courier, NOT via US Postal Service.
vii) Label all media with the following:
(1) Production date
(2) Bates range
(3) Disk number (1 of X), if applicable
(4) Name of producing party
(5) A unique production number identifying each production

4) All productions must be produced free of computer viruses.
5) All physical produced media must be encrypted. Encryption format must be agreed upon prior to production.
a) Data deliveries should be encrypted at the disc level.
b) Decryption keys should be provided separately from the data delivery via email or phone.
6) Passwords for documents, files, and compressed archives should be provided separately either via email or in a separate cover letter from the data.

B. Delivery Formats

1) General ESI Standards

All productions must follow the specifications outlined below:

<u>De-duplication</u>
De-duplication of documents should be applied across custodians (global); each custodian should be identified in the Custodian field in the metadata load file separated by semi-colon. The first name in the Custodian list should represent the original holder of the document.

<u>Bates Numbering Documents</u>
The Bates number must be a unique, sequential, consistently formatted identifier, i.e., an alpha prefix unique to each producing party along with a fixed length number, i.e., ABC0000001. This format must remain consistent across all productions. The number of

digits in the numeric portion of the format should not change in subsequent productions, nor should hyphens or other separators be added or deleted.

Document Retention / Preservation of Metadata

The recipient of a discovery request should use reasonable measures to maintain the original native source documents in a manner so as to preserve the metadata associated with these electronic materials as it existed at the time of the original creation.

Email Threading

The use of email threading for review is encouraged, but production of relevant email threads must include both inclusive and non-inclusive individual emails and attachments unless otherwise agreed to in advance.

2) Native and Image Production

In general, and subject to the specific instructions below: (1) produce electronic documents in their complete native/original format along with corresponding bates-labeled single page TIFF images (with the exception of large spreadsheets and/or text files, those files should be processed and a placeholder TIFF image indicating that they were produced natively provided); (2) scan and process all paper documents into single page TIFF images, OCR the images, and apply bates numbers to each page of the image; (3) produce fully searchable document level text for every produced document; and (4) produce metadata for every produced document in a data file that conforms to the specific instructions below.

a) Metadata File

All produced documents, regardless of their original file format, must be produced with the below-described metadata fields in a data file (.DAT).

i) The first line of the .DAT file must be a header row identifying the field names.
ii) The .DAT file must use the default delimiters (see **Table 1**)
iii) Date fields should be provided in the format: mm/dd/yyyy
iv) All attachments should sequentially follow the parent document/email.
v) All documents shall be produced in both their native/original form and as a corresponding bates-labeled single page TIFF image; provide the link to the original/native document in the NATIVELINK field.
vi) Produce extracted metadata for each document in the form of a .DAT file, and include the fields in **Table 2** (fields should be listed but left blank if not applicable):

b) Document Text

Searchable text of the entire document must be provided for every record, at the document level.

i) Extracted text must be provided for all documents that originated in electronic format.

Note: Any document in which text cannot be extracted must be OCR'd.

ii) For documents redacted on the basis of any privilege, provide the OCR text for unredacted/unprivileged portions.

iii) The text should be delivered as multi-page ASCII text files with the files named the same as the Bates_Begin field. Text files can be placed in a separate folder or included with the .TIFF files.

c) Linked Native Files

Copies of original email and native file documents/attachments must be included for all electronic productions.

i) Native file documents must be named per the BATES_BEGIN number (the original file name should be preserved and produced in the FILENAME metadata field).

ii) The full path of the native file must be provided in the .DAT file in the NATIVELINK field.

d) Images

i) Images should be single-page, Group IV TIFF files, at 300 dpi.

ii) File names should be titled per endorsed bates number.

iii) Color should be preserved when necessary to interpret the document.

iv) Bates numbers should be endorsed on the lower right corner of all images.

v) For documents partially redacted on the basis of any privilege, ensure the redaction box is clearly labeled "REDACTED".

e) Image Cross Reference File

i) The image cross-reference file is needed to link the images to the database. It is a comma-delimited file consisting of seven fields per line. There must be a line in the cross-reference file for every image in the database.

ii) See **Table 3** and **Table 4** for Image Cross Reference File fields and an example file.

3) PDF File Production

When approved, Adobe PDF files may be produced in lieu of TIFF images for scanned paper productions (metadata must also be produced in accordance with the instructions above):

a) PDF files should be produced in separate folders named by the Custodian.

b) All PDFs must be unitized at the document level, i.e. each PDF should represent a discrete document; a single PDF cannot contain multiple documents.
c) All attachments should sequentially follow the parent document.
d) All PDF files must contain embedded text that includes all discernible words within the document, not selected text only. This requires all layers of the PDF to be flattened first.
e) If PDF files are Bates endorsed, the PDF files must be named by the Bates range
f) The metadata load file listed in 2.a. should be included.

4) Transactional Data

If transactional data must be produced, further discussion must be had to ensure the intended export is properly composed. If available, a data dictionary should accompany the production; if unavailable, a description of fields should accompany transactional data productions. The following formats are acceptable:

- MS Access
- XML
- CSV
- TSV
- Excel (with prior approval)

5) Audio/Video/Electronic Phone Records

These instructions refer to the production of stand alone audio files such as those from call recording systems. Audio files that are attached to emails should be processed normally.

Audio files must be produced in a format that is playable using Microsoft Windows Media Player. Types of audio files that will be accepted include:

- Nice Systems audio files (.aud). AUD files offer efficient compression and would be preferred over both NMF and WAV files.
- Nice Systems audio files (.nmf).
- WAV Files
- MP3, MP4
- WMA
- AIF

Produced audio files must be in a separate folder compared to other data in the production. Additionally, the call information (metadata) related to each audio recording must be produced if it exists. The metadata file must be produced in

delimited text format (DAT, CSV, or TXT), using a tab or pipe delimiter. Field names must be included in the first row of the metadata file. Please note that the field names are case sensitive and should be created as listed below. The metadata must include, if available, the fields listed in **Table 5**.

The filename is used to link the metadata to the produced audio file. The file name in the metadata and the file name used to identify the corresponding audio file must match exactly.

Video files must be produced in a format that is playable using Microsoft Windows Media Player along with any available metadata. If it is known that the video files do not contain associated audio, indicate this in the accompanying transmittal letter. Types of video files accepted include:

- MPG
- AVI
- WMV
- MOV
- FLV

C. Production of Partially Privileged Documents

If a portion of any material called for by a discovery request is withheld based on a claim of privilege, those portions may be redacted from the responsive material as long as the following conditions are met.

a) If originally stored as native electronic files, the image(s) of the unredacted portions are submitted in a way that preserves the same appearance as the original without the redacted material (i.e., in a way that depicts the size and location of the redactions). The OCR text will be produced from the redacted image(s). Any redacted, privileged material should be clearly labeled to show the redactions on the tiff image(s). Any metadata not being withheld for privilege should be produced in the DAT file; any content (e.g., PowerPoint speaker notes, Word comments, Excel hidden rows, sheets or columns) contained within the native and not being withheld for privilege should be tiffed and included in the production.

b) If originally in hard copy form, the unredacted portions are submitted in a way that depicts the size and location of the redactions; for example, if all of the content on a particular page is privileged, a blank, sequentially numbered page should be

included in the production where the responsive material, had it not been privileged, would have been located.

APPENDIX A: TABLES

TABLE 1: DAT FILE DELIMITERS

Comma	¶	ASCII character (020)
Quote	þ	ASCII character (254)
Newline	®	ASCII character (174)

TABLE 2: DAT FILE FIELDS

Field Name	Description
Required Fields	
BATES_BEGIN	First Bates number of native file document/email
BATES_END	Last Bates number of native file document/email **The BATES_END field should be populated for single page documents/emails
ATTACH_BEGIN	First Bates number of attachment/family range
ATTACH_END	Last Bates number of attachment/family range
ATTACH_NAME	Populates parent records with original filenames of all attached records, separated by semi-colons.
PRIV	Indicate "YES" if document has a Privilege claim
ROG_NUM	Indicate Interrogatory number(s) document is responsive to. (ROG ##) **semi-colon should be used to separate multiple entries
DR_NUM	Indicate Document Request (DR ##) or Written Report number (WR ##) document is responsive to. **semi-colon should be used to separate multiple entries
RECORDTYPE	Email: Populate field as "E-Mail" Email Attachment: Populate field as "Attachment (E-mail)" Loose Native: Populate field as "E-Document" Other Attachment: Populate field as "Attachment" Scanned Paper: Populate field as "Paper"
CUSTODIAN	Individual(s) or department(s) from which the record originated **semi-colon should be used to separate multiple entries
FILENAME	Email: Filename of loose email or subject of non-loose email Non-email: original file name
PGCOUNT	Number of pages in document/email
MD5HASH	The 32 digit value representing each unique document

SOURCE	Email: Path to email container and email container name Non-email: Original path to source archive folder or files
FOLDERPATH	Email: Folder path within email container Non-email: Folder path to file
DATE_CREATED	Date and time the electronic file was created ** format example: "04/20/2021 5:15 PM" or "04/20/2021 17:15"
DATE_MOD	Date and time an electronic file was last modified ** format example: "04/20/2021 5:15 PM" or "04/20/2021 17:15"
PRINT_DATE	Date and time the document was last printed ** format example: "04/20/2021 5:15 PM" or "04/20/2021 17:15"
FILE_SIZE	Size of native file document/email in KB
FILE_EXT	The file extension representing the email or native file document
AUTHOR	Email: (empty) Non-email: Author of the document
SUBJECT(EDOC)	Subject metadata from electronic files (non-email)
TITLE	Title metadata from electronic files (non-email)
COMPANY	Company (organization) metadata from electronic files
NATIVELINK	Hyperlink to the email or native file document **The linked file must be named per the BATES_BEGIN Number
TEXTPATH	Contains path to OCR/Extracted text file that is titled after the document BATES_BEGIN
Additional Fields for Email Productions	
FROM	Sender of email
TO	Recipient(s) of email **semi-colon should be used to separate multiple entries
CC	Carbon copy recipient(s) **semi-colon should be used to separate multiple entries
BCC	Blind carbon copy recipient(s) **semi-colon should be used to separate multiple entries
SUBJECT(EMAIL)	"Subject" line of the email
DATE_SENT	Date and time that the email message was sent.
DATE_RECVD	Date and time that the email message was received.
TIME_ZONE	Time Zone processed in
PARENT_ID	Populated only for email attachments, this field will display the Image Tag field value of the attachment record's parent.

TABLE 3: IMAGE CROSS REFERENCE FILE FIELDS

Field Title	Description
ImageID	The unique designation use to identify an image.
	Note: *This imageID key* ***must*** *be a unique and fixed length number. This number will be used in the.DAT file as the ImageID field that links the database to the images. The format of this image key must be consistent across all productions. We recommend that the format be an eight digit number to allow for the possible increase in the size of a production.*
VolumeLabel	Optional
ImageFilePath	The full path to the image file.
DocumentBreak	The letter "Y" denotes the first page of a document. If this field is blank, then the page is not the first page of a document.
FolderBreak	Leave empty
BoxBreak	Leave empty
PageCount	Optional
	**This file should not contain a header row.*

TABLE 4: IMAGE CROSS REFERENCE FILE SAMPLE

IMG0000001,OPTIONALVOLUMENAME,E:\001\IMG0000001.TIF,Y,,,3
IMG0000002,OPTIONALVOLUMENAME,E:\001\IMG0000002.TIF,,,,
IMG0000003,OPTIONALVOLUMENAME,E:\001\IMG0000003.TIF,,,,
IMG0000004,OPTIONALVOLUMENAME,E:\001\IMG0000004.TIF,Y,,,1
IMG0000005,OPTIONALVOLUMENAME,E:\001\IMG0000005.TIF,Y,,,2
IMG0000006,OPTIONALVOLUMENAME,E:\001\IMG0000006.TIF,,,,

TABLE 5: AUDIO METADATA FIELDS

Field Name	Description
AgentName	Name of agent/employee
AgentId	Unique identifier of agent/employee
Group	Name for a collection of agents
Supervisor	Name of the Agent's supervisor
Site	Location of call facility
DNIS	Dialed Number Identification Service, identifies the number that was originally called
Extension	Extension where call was routed
CallDirection	Identifies whether the call was inbound, outbound, or internal
CallType	Purpose of the call

Duration	Duration of call
CustomerId	Customer's identification number
CustomerCity	Customer's city of residence
CustomerState	Customer's state of residence
CallDateTime	Date and start time of call (MM/DD/YYYY HH:MM:SS)
CustomerName	Name of person called
FileName	Filename of audio file
BatesBegin	Unique number of the audio file
CalledPartyNumber	The call center or phone number called
CallSize	File size of audio file
CallService	Call service code
MD5Hash	The 32 digit value representing each unique document
DocReq	Document request number to which the file is responsive
Custodian	Individual(s) or department(s) from which the recording originated
FolderPath	Folder path of the audio file in the original source
Source	Original path to where the source file resided
Timezone	The time zone of the original call
GroupID	A unique group identifier for grouping multiple calls
Codec	Encoding/decoding of the audio digital stream
Bitrate	The number of bits that are conveyed or processed per unit of time

Supported Date Format	**Example**
mm/dd/yyyy hh:mm:ss am/pm	01/25/1996 10:45:15 am

APPENDIX B: PROHIBITED FILE TYPES FOR EXTRANET

.ade	.mar	.vbe
.adp	.mas	.vbs
.app	.mat	.vsmacros
.asp	.mau	.vss
.bas	.mav	.vst
.bat	.maw	.vsw
.cer	.mda	.ws
.chm	.mdb	.wsc
.cmd	.mde	.wsf
.com	.mdt	.wsh
.cpl	.mdw	
.crt	.mdz	
.csh	.msc	
.dll	.msi	
.exe	.msp	
.fxp	.mst	
.gadget	.ops	
.hlp	.pcd	
.hta	.pif	
.inf	.prf	
.ins	.prg	
.isp	.pst	
.its	.rar	
.js	.reg	
.jse	.scf	
.ksh	.scr	
.lnk	.sct	
.mad	.shb	
.maf	.shs	
.mag	.tmp	
.mam	.url	
.maq	.vb	